REMARKS

Priority Claim

Applicants again request that the Office acknowledge the claim to priority made in the preliminary amendment received by the Office on December 22, 2004.

Status of Pending Claims

Claims 1 – 66 were examined, and all were rejected.

Claims 54 – 59 have been canceled.

Claims 1 – 53 and 60 – 66 remain pending.

Claims 1, 26, 33, 43, 44, 52, and 60 have been amended to recite preventing access by remote devices to cryptographic keys used by the key server to perform cryptographic operations. Support is found at least at p. 7, ll. 3 – 23 of the application.

Claims 8 and 9 are amended to correct minor informalities.

No new matter has been added to the application by these amendments.

Regarding Examiner's Comments on Response to Arguments

The Examiner has taken the position that Applicants' argument presented on pages 16 – 20 of the response to the previous Office action "mainly argues that the prior art of record does not explicitly disclose at least one unique identifier for identifying at least one key for performing transformation." Applicants respectfully point out that, although Applicants did make that argument, it accounted for only about one tenth of the space devoted to arguments presented against the claim rejections. Consequently, applicants understand that the Examiner's lack of comments with regard to the remaining arguments indicate tacit approval of those arguments, in accordance with applicable case law and MPEP 707.07(f):

> The importance of answering applicant's arguments is illustrated by In re Herrmann, 261 F.2d 598, 120 USPQ 182 (CCPA 1958) where the applicant urged that the subject matter claimed produced new and useful results. The court noted that since applicant's statement of advantages was not questioned by the examiner or the Board of Appeals, it was constrained to accept the statement at face value and therefore found certain claims to be allowable. See also In re Soni, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995) (Office failed to rebut applicant's argument).

Accordingly, Applicants respectfully request that allowable subject matter be explicitly recognized in the claims to which Applicants' unanswered arguments pertain. Alternatively, Applicants respectfully maintain all of the unanswered arguments presented in the response to the previous Office action by reference to that response as if those arguments were again fully set forth herein, and respectfully request a response to those arguments, so Applicants can consider and address any reasons that may be presented for maintaining the rejections.

Moreover, the Examiner admits that "the prior art does not explicitly mention the use of identifiers to establish cryptographic keys," but contends the prior art discloses negotiating keys to be used to establish secure communication "and also for data encryption," citing Berson, 10:40 – 57 for support. That explanation appears to recognize the differences disclosed in the specification and in Berson between 1) establishing keys for secure communication, and 2) establishing different keys for encryption operations. However, it also suggests that the rejection is based on incorrect interpretations of both the teachings of Berson and the teachings of the current specification.

The cited location in Berson discloses that a first key is established between the client and server. That key is used to secure communications between the client and server, such as by establishing a secure tunnel (Berson, 10: 44 – 46). Thereafter, encrypted information is received at the server from the client (id., 46 – 48). "A second key also can be sent to the server from the client," (id., 49 – 50). That second key is for the server to use in encryption operations *distinct* from the operations performed in connection with the secure tunnel. "Once the work [i.e., the cryptographic operation] has been performed, it (i.e., the result of the cryptographic operation) is sent to the client from the server," (id., 50 – 51). Thus, a secure tunnel is established between the client and the server. Thereafter, the client sends to the server data that requires a cryptographic operation and the key needed to perform the operation, to offload the processing burden associated with the operation from the client to the server. The server returns to the client the operated-on data.

In contrast, the present disclosure teaches that keys for cryptographic operations are provided to the cryptographic service engine by a secure key provider for the engine to use in cryptographic operations on data provided by the client, while preventing access to those keys by

the client. Berson does not disclose, suggest, or render obvious preventing access to cryptographic keys by a client.

Request for reconsideration of the finality of the rejection of the last Office action

In view of the remarks presented above, the Examiner is respectfully requested to reconsider the finality of the rejection of the last Office action, and address the unanswered arguments presented in response to that action. Applicants should be afforded the opportunity to consider the value of any allowable subject matter identified, and to consider and address any reasons that may be presented for maintaining the rejections.

Claim Rejections - 35 USC §102

Claims 1 – 24 stand rejected under 35 U.S.C. § 102(b) as allegedly anticipated by Berson et al. (U.S. patent 7,051,199). The rejection is traversed with regard to the claims as currently presented.

The claims are directed to a network attached encryption server for providing cryptographic services to remotely hosted applications. The encryption server can thereby offload the associated cryptographic processing burden from the remote hosts running the applications. The server can also provide such services for a plurality of such remote hosts, as well as centralized management of the encryption services provided by the encryption server. Moreover, the encryption server has secure access to the cryptographic keys used to perform cryptographic operations, whereas the remote hosts are prevented from accessing those cryptographic keys. For example, the cryptographic keys can be stored in a hardware security module (HSM), and may themselves be encrypted and further secured, such as by requiring the use of *k* out of *n* smart cards to access the keys (p. 7, ll. 7 – 22). Accordingly, an unsecure condition on a host, such as a security breach by a malicious hacker or a disgruntled employee, cannot compromise the security of the keys.

In contrast, Berson teaches a system including a cryptographic server providing cryptographic services to clients, in which the clients themselves provide the keys to be used in cryptographic operations. In Berson, "a first key is established, and a tunnel is generated on the network [between the client and the server]. Thereafter, information is received at the server

from the client utilizing the tunnel. Such information is encrypted by the client using the first key." Berson, 3:6 – 9. Information is then sent from the client to the server through the tunnel, including keys, messages and ciphertext (id., 3:15 – 17). In other words, in Berson the keys used by the server to perform cryptographic operations are provided by the client of the server, and the client is not prevented from accessing those keys. Although Berson briefly discloses embodiments in which it is not clear where the keys used for cryptographic operations come from (id., 10:14 – 21), and an embodiment in which "the cryptoserver already knows the client's private key," (id., 12:5 – 7), it is clear that in the "preferred embodiment" the cryptographic keys are provided by the client (id., 12:3 – 4). Moreover, nowhere does Berson disclose or remotely suggest that clients are prevented from accessing the keys used by the cryptoserver to perform cryptographic operations. Even in the embodiment in which the cryptoserver already knows the client's private key, it is implied that the cryptoserver first obtained the client's private key from the client, and stored it for later use (id., 12:6 – 8).

Claim 1 recites a cryptographic service engine in bi-directional communication with a secure key provider providing access by the cryptographic service engine to cryptographic keys, and preventing access by remote devices to the cryptographic keys, wherein client cryptographic service requests comprise an identifier for identifying the cryptographic key to use for cryptographic operations, data to be operated on, and instructions for how the cryptographic service engine should operate on the data. Berson does not disclose or suggest those features. Therefore, Berson does not anticipate claim 1, and the section 102 rejection of claim 1 cannot be sustained. Claims 2 – 24 depend from claim 1, and contain all of its features. Accordingly, without prejudice to their own individual merits, those claims are allowable for at least the same reasons claim 1 is allowable.

In addition, regarding claim 21, the Examiner contends Berson 6:44 – 67 discloses claimed elements including a hardware security module bi-directionally coupled to a database and suitable for storing private keys, and a smart card interface device. However, Berson does not disclose those features, at the cited location or elsewhere. The only feature claimed in claim 21 that could be reasonably construed to read on that portion of Berson is the separately recited "cryptographic accelerator card bi-directionally coupled to said databus." Because Berson does not disclose all of the features of claim 21, the rejection of claim 21 is not supported, and claim

21 is allowable for that reason as well. Claims 22 – 24 depend from claim 21, and are allowable for at least the same reasons.

Based on the remarks presented above, reconsideration and withdrawal of the section 102 rejection of claims 1 – 24 are respectfully requested.

Claim Rejections - 35 USC §103

Claims 25 – 66 stand rejected under 35 U.S.C. § 103(b) as allegedly being unpatentable over Benson. Claims 54 – 59 are canceled, mooting the rejection as to those claims. The rejection is traversed with regard to the remaining claims as currently presented.

Regarding claim 25, the Examiner admits Berson does not disclose applying the secret sharing scheme claimed, but contends it would have been obvious to add that feature to Berson, i.e., using "k-out-of-n" smart cards inserted into the cryptographic key server. However, the Examiner's rationale for extending Berson is to use such a scheme "when multiple clients interface with a security server," which suggests that the Examiner does not fully appreciate how such a scheme works, because it has nothing to do with supporting multiple clients, but rather with providing greater protection for the cryptographic keys. The claimed scheme would be used even if only one client were present. Accordingly, the rationale suggested by the Examiner for extending Berson is inapposite, and the rejection of claim 25 should be withdrawn.

Regarding claims 26 – 66, the Examiner contends they encompass the same or similar scope as claims 1 – 25, and are rejected based on the same reasons set forth in the rejections of claims 1 – 25. Applicants respectfully disagree, and note that at least some of claims 26 – 66 comprise features not found in claims 1 – 25, nor are they disclosed, suggested, or rendered obvious by Berson. For example, claims 65 – 66 depend from claim 1 and comprise features not found in claim 1 or its other dependents, nor in Berson. Furthermore, Berson does not provide at least claimed features pertaining to an application's use of a cryptographic API (claims 27, 32, 42), Java Cryptographic Extensions (clam 29), a Cryptographic Service Provider and an API implemented as a DLLs (claim 30), an API exposed via MS-CAPI (claim 31), establishing a set of keys on a network key server (claim 33), determining authorization privileges in connection with providing encryption services over a network (claims 39, 40), tracking requests for cryptographic services (claim 41), storing sensitive data only in encrypted form (claim 47),

controlling access to keys stored in a cryptographic key server (claims 48 – 50), a cryptographic appliance comprising a hardware security module and a smart card interface (claim 51), and intercepting and encrypting data en route to an application server (claim 53).

As noted above, independent claims 27, 32, 33, 42, 48, 51, and 53 comprise features that are not disclosed, suggested, or rendered obvious by Berson. Therefore, the section 103 rejection of those claims and their dependents is not supported, and should be withdrawn. In addition, independent claims 26, 43, 44, 52, 54, and 60 have been amended to include a key server that prevents access to stored cryptographic keys by a remote device. As noted previously in connection with claim 1, that feature is not disclosed, suggested, or rendered obvious by Berson. Therefore, the section 103 rejection of those claims and their dependents is also not supported, and should be withdrawn.

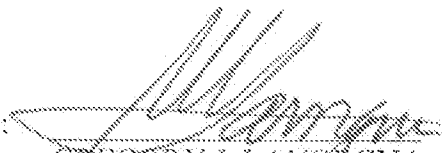
Based on the remarks presented above, reconsideration and withdrawal of the section 103 rejection of claims 25 – 53 and 60 – 66 are respectfully requested.

Conclusion

No other matters remain. In view of the foregoing amendment and remarks, Applicants respectfully submit that the present application, including claims 1 – 53 and 60 – 66, is in condition for allowance and an early notice of allowance is respectfully requested. The Examiner is invited to contact the undersigned or his associate Michael Berman, Esq. at 215-988-1164 if that would expedite prosecution.

Respectfully submitted,

THOMAS FOUNTAIN, *et al.*

BY: 

GREGORY J. LAVORGNA
Registration No. 30,469
Drinker Biddle & Reath LLP
One Logan Square, Ste. 2000
Philadelphia, PA 19103-6996
Tel: 215-988-3309
Fax: 215-988-2757
Attorney for Applicant